

**LECTURE NOTES**  
**Fundamentals of Group Theory**

Dr. Muhammad Awais Yousaf

Department of Mathematics  
The Islamia University of Bahawalpur, 63100 Bahawalpur

# DEFINITIONS AND SOME IMPORTANT GROUPS

## 1. HISTORICAL BACKGROUND

Almost all the great mathematicians have ventured to devise a general method for finding the solutions of equations of all degrees, but none of them succeeded until the time of Khwarizmi. It was in his time that some general methods began to appear in the mathematical literature. Ancient records show that Khwarizmi, Omar Khayyam, Abu Kamil and Abu Wafa succeeded in devising the first known general algebraic methods for finding the solutions of linear and quadratic equations. (The reader is referred to my book *Mathematics: The Islamic Legacy*, Centre for the Study of Civilization of Central Asia, 1990). It was not until the Renaissance period, that is, from 1450 to 1700, that algebraic solutions for the cubic and also the quartic equation were found. Later, in the 18<sup>th</sup> century, L. Euler first worked on the idea that the problem of the quintic equation could be reduced to that of solving a quartic. J. L. Lagrange made the same attempt. The failures of such able mathematicians led to the belief that such a reduction might be impossible. It was C.F. Gauss and P. Ruffini in the early 19<sup>th</sup> century who first attempted to prove that the *quintic* could not be solved by algebraic methods. N.H. Abel's work on these lines inspired E. Galois who then discovered that an irreducible algebraic equation is soluble by radical if and only if a certain group of permutations of its roots is soluble. From this time, group theory took explicit form and has since played a fundamental role in all fields of mathematics. A.I. Cauchy studied the group of permutations of roots for its own interest but the complete description of the relationship between groups and algebraic equations was first given by E. Galois. Later C. Jordan developed a detailed exposition of the theory due to N.H. Abel and E. Galois. Up to that time, a group meant a permutation group; the axiomatic definition of a group was given by A. Cayley and I. Kronecker. F. Klein emphasised the significance of group theory in geometry and S. Lie developed the theory of Lie groups in the 1880s. In 1897, W. Burnside published his classical book on group theory and through it inspired the British group theorists. Since 1896, F.G. Frobenius and others have developed the theory of representation of groups by matrices. By that time, the theory of finite groups had acquired all its essential features. Amongst the branches of abstract algebra, the theory of groups was the first to develop; it led to the progress of abstract algebra in the 1930s. Since the later half of that decade, the theory of finite groups has been developed further; there has been an increased interest in the theory and many significant results have been obtained, especially since 1955.

## 2. DEFINITION OF A GROUP AND SOME EXAMPLES

The multiplicity of algebras invented in the 19<sup>th</sup> century might have given mathematics a centrifugal tendency had it not been for the development of certain structural concepts. One of the most important of these was the notion of a group, the unifying role of which in geometry will be highlighted in the following discussion. In algebra, the group concept was no doubt the most important force making for cohesiveness, and it was an essential factor in the rise of abstract views. No one was

responsible (as we have mentioned in Section 1.1) for the rise of the group idea, but the figure that loomed largest in this connection was that of the man who gave the concept its name in 1830, the young E. Galois, who died tragically before the age of twenty one.

Let us see what we mean by a group. A set of elements is said to form a group with respect to a given operation if

- (i) the set is closed under the operation;
- (ii) the set contains the identity element with respect to the operation;
- (iii) for every element in the set there is an inverse element with respect to the operation; and
- (iv) the operation is associative.

The elements of the set can be numbers (as in arithmetic), points (as in geometry), or anything at all. The operation can be arithmetic (such as addition or multiplication) or geometric (such as a rotation about a point or an axis), or any other rule for combining two elements of a set (such as two transformations) to form a third element in the set. Throughout this book, without any loss of generality, we will use multiplication as the operation. If  $a$  and  $b$  are elements of a group then their combination will be denoted by  $ab$  or simply by  $ab$ .

Since mathematics is now built on a set theoretic foundation, at least for expository purposes. It is of some importance to see that the definition of a group can be formulated using only the notions of set theory.

A set  $G$  is called a group if

- (i) for every,  $a, b \in G, ab \in G$ ;
- (ii) there exists  $e \in G$  such that  $ae = ea = a$  for every  $a \in G$ ;
- (iii) for every  $a \in G$  there exists  $a' \in G$  such that  $a'a = aa' = e$ ;
- (iv) for every  $a, b, c \in G$ ,  $(ab)c = a(bc)$ .

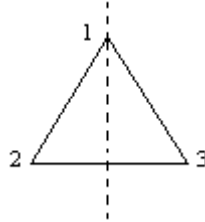
The element  $e \in G$  is called the identity element. Throughout this book we will denote it by 1. The element  $a'$  is called the inverse of  $a$  (or vice-versa). Note that in a group the inverses and identity are always unique.

In mathematics especially, examples are a good means of making the definitions and theorems conceptually clearer. Examples, although are particularities, they are suggestive and quite often lead to generalities. In a course like this, one cannot underestimate their significance. In this chapter, we have explained definitions and theorems through examples, which not only give insight into the theory but also are significant in their own right.

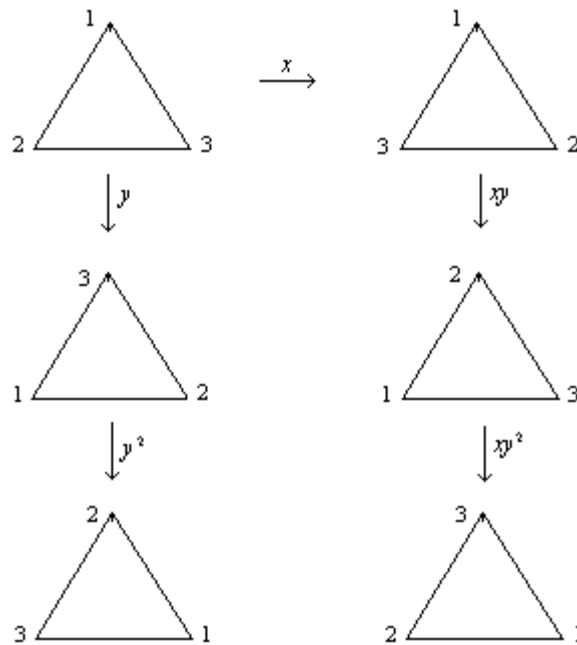
Let us now pass on to examples of groups.

### Example 1.2.1

We consider an equilateral triangle in a plane and rotate it in such a way that it appears not to have moved. Let us rotate the triangle with vertices 1, 2 and 3 about vertical axis passing through the centre of the triangle and perpendicular to the base.



Denote this rotation by  $x$ . Now rotate the triangle about an axis perpendicular to the plane of the triangle in a counter clockwise direction through  $120^\circ$ . Let us denote this rotation by  $y$ . By  $xy$  we shall mean the rotation  $x$  followed by  $y$ . Similarly, by  $y^2$  we shall mean the rotation  $y$  followed by  $y$ . In the following, let us consider the rotations:  $x, x^2, y, y^2, xy, xy^2$



In this way, we get six distinct positions of the triangle. The set  $G = \{x, x^2, y, y^2, xy, xy^2\}$  is a group. Before we prove this we shall note that the rotations  $x^2, y^3$  and  $(xy)^2$  do not change the initial position of the triangle. We denote such a rotation by 1 and call it the identity. Thus  $x^2 = 1, y^3 = 1$  and  $(xy)^2 = 1$ .

The following Cayley table confirms that  $G$  is a group. It is important to note that this group  $G$  is denoted by a standard notation  $S_3$ .

|        | 1      | $x$    | $y$    | $y^2$  | $xy$   | $xy^2$ |
|--------|--------|--------|--------|--------|--------|--------|
| 1      | 1      | $x$    | $y$    | $y^2$  | $xy$   | $xy^2$ |
| $x$    | $x$    | 1      | $xy$   | $xy^2$ | $y$    | $y^2$  |
| $y$    | $y$    | $xy^2$ | $y^2$  | 1      | $x$    | $xy$   |
| $y^2$  | $y^2$  | $xy$   | 1      | $y$    | $xy^2$ | $x$    |
| $xy$   | $xy$   | $y^2$  | $xy^2$ | $x$    | 1      | $y$    |
| $xy^2$ | $xy^2$ | $y$    | $x$    | $xy$   | $y^2$  | 1      |

Note that 1 is the identity element of  $G$  and the inverse of:

$$\begin{array}{lll}
 x & \text{is} & x \\
 y & \text{is} & y^2 \\
 xy & \text{is} & xy \\
 xy^2 & \text{is} & xy^2
 \end{array}$$

### Example 1.2.2

The sets  $Z$ ,  $R$ ,  $Q$  and  $C$  are groups under the operation of addition.

### Example 1.2.3

The non-zero elements of  $R$ ,  $Q$  and  $C$  form groups under the operation of multiplication.

### Example 1.2.4

Let  $X$  be a non-empty set and  $Sym(X)$  denote the set of all bijections from  $X$  onto from  $X$  onto itself. Then  $Sym(X)$  is a group under the mapping composition:  $(x)f \circ g = ((x)f)g$  for every  $x \in X$  and  $f, g \in Sym(X)$ .

### Example 1.2.5

The set of all non-singular  $n \times n$  matrices with entries from the real line  $R$ , forms a group under the usual matrix multiplication. This group is known as the general linear group of degree  $n$  over  $R$  and is denoted by  $GL(n, R)$ .

It is an important group with wide uses. We will discuss some of its characteristics in Chapter 5.

**Example 1.2.6**

The solution of equation  $x^4 - 1 = 0$  in  $C$ , where  $C$  contains the complex numbers, form the group  $\{1, -1, i, -i\}$  under multiplication.

Note that in example 1.2.1,  $xy \neq yx$ . That is, the rotation  $x$  followed by  $y$  is not equal to the rotation  $y$  followed by  $x$ . A group  $G$  in which  $ab = ba$  for all  $a, b$  in  $G$ , is of special interest in group theory. It is called an Abelian group. The name is in honour of a young Norwegian mathematician N.H. Abel, whose work in 1827 and 1828 initiated the study of such groups.

**Example 1.2.7**

The set of all  $m \times n$  matrices with entries from sets  $R$ ,  $Q$  or  $C$  forms an Abelian group under matrix addition.

**Example 1.2.8**

Suppose  $G$  contains only the real numbers 1 and -1. Then  $G$  is an Abelian group under the operation of multiplication.

**Example 1.2.9**

Let  $n$  be a positive integer and a relation ' $\equiv$ ' is defined in  $Z$  as  $a \equiv b \pmod{n}$  if and only if  $n$  divides  $a - b$ . The relation ' $\equiv$ ' is an equivalence relation and it partitions  $Z$  into non-empty, disjoint equivalence classes. By  $\overline{a}$  we mean a class  $\{x \in Z : x \equiv a \pmod{n}\}$ . If we define addition of classes by  $\overline{a} + \overline{b} = \overline{a + b}$ , then  $Z_n$ , the set of equivalence classes, forms an Abelian group under this operation of addition.

The size of a group plays an important role in the theory of groups. A group is called finite if it has a finite number of elements; otherwise it is called an infinite group. The examples 1.2.1, 1.2.6, 1.2.8, and 1.2.9 are the examples of finite groups whereas the examples 1.2.2, 1.2.3, 1.2.5 and 1.2.7 are examples of infinite groups. The number of elements in a group  $G$  is called the order of  $G$  and is denoted by  $|G|$ . For instance, in examples 1.2.1 and 1.2.6 the groups are of orders 6 and 4 respectively.

There are several ways in which a group can be expressed. In the next section we explain a technique for constructing groups. The groups expressed by means of this technique arise in such theories as knot theory, automorphic functions, topology and geometry.

### 3. GENERATORS AND RELATIONS

One of the useful ways of presenting a group is called a "generators and relations description" or a "finite presentation". It is a very useful way of describing a group. It is

useful in the sense that we can derive information about a group from a presentation of it. We explain the method through example 1.2.1.

Notice that every element of  $S_3$  is an expression in  $x, y$  or their powers. Such expressions are called 'words'. For example, an element  $xyx^2y^3x^3y^5x^5$  of  $S_3$  is a word in  $x, y$  and  $x^5$  is short for  $xxxxx$ . We write 1 for the word with no symbols in it. It is called empty word. For instance,  $x^2 = 1$  would mean that  $x^2$  could be replaced by 1. Thus, by using  $x^2 = 1$  and  $y^3 = 1$ , the word  $xyx^2y^3x^3y^5x^5$  can be replaced by the word  $yx$ . The equations  $x^2 = 1$ ,  $y^3 = 1$  and  $(xy)^2 = 1$  are called relations and  $x, y$  are called generators of  $S_3$ . Hence it is quite logical to represent  $S_3$  as  $\langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ . Since the number of generators and relations in the group is finite, the presentation is called a finite presentation. Note the notation  $\langle \dots : \dots \rangle$ . The generators are written on the left of colon and the relations on the right. More generally, the expression  $\langle a, b, c, \dots : R_1, R_2, \dots \rangle$  denotes the group generated by the symbols  $a, b, c, \dots$  subject to the relations  $R_1, R_2, \dots$  according to the procedure defined above. In the general case some words will involve symbols  $a^{-1}, b^{-1}, \dots$  and their powers. Sometimes, instead of this, we use relations of the form  $a^r = 1$ , where  $r > 0$ ,  $a^{-1} = a^{r-1}$ . It must be emphasised that the treatment here is informal.

Let us consider a few examples for illustration.

### Example 1.3.1

A group of four elements  $1, x, y, xy$  can be written as  $\langle x, y : x^2 = y^2 = (xy)^2 = 1 \rangle$ . This is the smallest, non-trivial Abelian group generated by more than one generator. It is called Klein 4-group and is usually denoted by  $V_4$ .

### Example 1.3.2

Suppose  $\Delta_n$  denotes a regular polygon with  $n \geq 3$  number of vertices. The  $n$  rotations of  $\Delta_n$  through angles,  $0, 2\pi/n, \dots, 2(n-1)\pi/n$ , together with the  $n$  reflections about the line joining opposite vertices of  $\Delta_n$  and the lines joining mid-points of opposite edges of  $\Delta_n$  (if  $n$  is even) or about the lines joining vertices of  $\Delta_n$  to mid-points of opposite (if  $n$  is odd) form a group. This group is called a Dihedral group of order  $2n$  and is denoted by  $D_n$  or  $D_{2n}$ . We will use the notation  $D_{2n}$ .

If  $a$  denotes the rotation about the centre of  $\Delta_n$  through an angle  $2\pi/n$  and  $b$  any one of the  $n$  reflections in  $D_{2n}$  then it is easy to show that  $D_{2n} = \langle a, b : a^n = b^2 = (ab)^2 = 1 \rangle$ . In the set tabular form  $D_{2n}$  is the group  $\{1, a, a^2, a^3, \dots, a^{n-1}, b, ab, a^2b, \dots, a^{n-1}b\}$ . Note that  $D_{2n}$  is independent of the size of  $\Delta_n$  and

of its position in the plane. It depends only upon the number of edges which is  $n$ . Since  $a^{-1} \neq a$ , the group  $D_{2n}$  is non-Abelian.

### Example 1.3.3

Consider the group of equivalence classes of integers modulo a prime number  $p$ , that is,  $Z_p$  under addition. Then  $Z_p = \langle 1 \rangle$ , where 1 is the generator of  $Z_p$ .

The following group was discovered by Sir W.R. Hamilton, in 1843. He always considered his discovery of quaternions as his greatest achievement. This discovery gave tremendous freedom to mathematicians to build algebras that need not satisfy the restrictions imposed by the so-called 'fundamental laws'.

### Example 1.3.4

If  $j = \begin{bmatrix} j & 0 \\ 0 & -1 \end{bmatrix}$  and  $k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ , and the complex number  $j$  is identified with the matrix  $jk = \begin{bmatrix} 0 & j \\ j & 0 \end{bmatrix}$  then the group  $\{1, j, j^2, j^3, k, k^2, k^3, jk\} = \{1, i, j, k, -1, -j, -k\}$  is denoted by  $Q_8$  and is called the quaternion group of order 8. Note that  $1, j, k$  satisfy the relations  $j^2 = j^2 = k^2 = ijk = -1, j = jk = -kj, j = ki = -ik$  and  $k = ij = -ij$ . The group  $Q_8$  has the presentation  $\langle jk : j^4 = k^4 = 1, jk = kj^3 \rangle$ . The group  $Q_8$  is non-Abelian.

In order to find a finite presentation of a group we need to know the generators and the relations they satisfy. For this, we need to know the order of the generators. In the next section, we explain the order of an element of a group and describe some useful characteristics related to this notion.

## 4. ORDER OF AN ELEMENT OF A GROUP

Let  $G$  be a group and  $x$  be an element of  $G$ . Then the smallest positive integer  $n$  for which  $x^n = 1$  is called the order of the element  $x$ . If no such  $n$  exists,  $x$  is said to have infinite order. The only element whose order is 1 is the identity element.

The order of an element must be distinguished from the order of the group. The order of an element  $x$  of a group  $G$  will be denoted by  $ord(x)$ .

Let us consider a few examples to illustrate this notion.

### Example 1.4.1

Consider the Klein 4-group  $V_4$ . The order of  $V_4$  is 4 and each element of  $V_4$ , except the identity element 1, is of order 2. That is  $ord(x) = 2, ord(y) = 2, ord(xy) = 2$  and  $|V_4| = 4$ , where  $V_4 = \langle x, y : x^2 = y^2 = (xy)^2 = 1 \rangle$ .



**Example 1.4.2**

In the group  $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ , obviously,  $\text{ord}(x) = 2$ ,  $\text{ord}(y) = 3$ ,  $\text{ord}(xy) = 2$ ,  $\text{ord}(y^2) = 3$ ,  $\text{ord}(xy^2) = 2$  and  $|S_3| = 6$ .

**Example 1.4.3**

If we rotate a regular polygon of  $n$  vertices about its center through an angle  $2\pi/n$  then the rotation is an element of order  $n$ .

In example 1.4.2, we have seen that  $|S_3| = 6$ . and orders of non-identity elements are either 2 or 3. It suggests that order of an element of a group is a factor of the order of group. Later we will have a general result in which a relationship will be established between the order of a group and the orders of its elements. But, first, in the following we collect together some results on the orders of elements in a finite group. These results will prove useful in our subsequent work.

**Theorem 1.4.4**

Let  $G$  be a group and  $a \in G$ . Then  $\text{ord}(a) = \text{ord}(a^{-1})$ .

**Proof.**

Suppose  $\text{ord}(a) = n$  and  $\text{ord}(a^{-1}) = m$ . Then  $(a^{-1})^n = (a^n)^{-1} = (1)^{-1} = 1$  implies that  $m \leq n$ . Similarly,  $(a)^m = ((a^{-1})^{-1})^m = ((a^{-1})^m)^{-1} = (1)^{-1} = 1$  implies that  $n \leq m$ . The two inequalities imply that  $n = m$ . Hence  $\text{ord}(a) = \text{ord}(a^{-1})$ .

**Theorem 1.4.5**

If  $G$  is a group and  $a \in G$  has order  $n$ , then  $a^m = 1$  if and only if  $n$  divides  $m$ .

**Proof.**

If  $n$  divides  $m$  then there exists  $q \in \mathbb{Z}$  such that  $m = nq$ . Thus  $a^n = 1$ , implies that  $a^m = a^{nq} = (a^n)^q = (1)^q = 1$ .

Conversely, suppose that  $a^m = 1$ . Since  $n$  is the least positive integer such that  $a^n = 1$ , therefore  $n \leq m$ . If  $n$  does not divide  $m$  then there exist unique integers  $q$  and  $r$  such that  $m = nq + r$  where  $0 < r < n$ . Now  $a^m = 1$  implies that  $1 = a^{nq+r} = a^{nq} a^r = (a^n)^q a^r = (1)^q a^r = a^r$ . That is,  $a^r = 1$  where  $r < n$ . But this contradicts the hypothesis that  $n$  is the least positive integer such that  $a^n = 1$ . Thus our assumption that  $n$  does not divide  $m$  is false. Hence the theorem.

**Theorem 1.4.6**

If  $G$  is a group and  $b = x^{-1}ax$  for  $a, b, x \in G$ , then  $\text{ord}(a) = \text{ord}(b)$ .

**Proof.**

Let  $\text{ord}(a) = n$  and  $\text{ord}(b) = m$ . Then

$$\begin{aligned} b^n &= (x^{-1}ax)^n = (x^{-1}ax)(x^{-1}ax)\dots(x^{-1}ax), \text{ } n\text{-times} \\ &= x^{-1}a(xx^{-1})a(xx^{-1})\dots x^{-1}a(xx^{-1})ax \\ &= x^{-1}a^n x. \end{aligned}$$

But  $a^n = 1$  and so  $b^n = x^{-1}1x = xx^{-1} = 1$ . This shows that  $m \leq n$ . Similarly  $a^m = (xbx^{-1})^m = xb^m x^{-1} = x^1 x^{-1} = xx^{-1} = 1$  implies that  $n \leq m$ . The two inequalities imply that  $n = m$ . Hence  $\text{ord}(a) = \text{ord}(b)$ .

#### Theorem 1.4.7

Let  $G$  be a group and  $a, b \in G$  such that  $\text{ord}(a) = n$ ,  $\text{ord}(b) = m$  where  $n, m$  are relatively prime. If  $ab = ba$  then  $\text{ord}(ab) = mn$ .

**Proof.**

Since  $ab = ba$ ,  $(ab)^{mn} = a^{mn}b^{mn}$ . But  $\text{ord}(a) = n$  and  $\text{ord}(b) = m$  imply that  $a^{mn}b^{mn} = 1$ . That is  $(ab)^{mn} = 1$ . Thus  $\text{ord}(ab)$  divides  $mn$ . Suppose  $\text{ord}(ab) = m_1 n_1$  where  $m_1$  divides  $m$  and  $n_1$  divides  $n$ . Then  $m_1$  and  $n_1$  are relatively prime and we may write  $m = km_1$  and  $n = ln_1$  for some positive integers  $k$  and  $l$ . Thus  $1 = (ab)^{m_1 n_1} = (ab)^{km_1 ln_1} = (ab)^{mn} = a^{mn}b^{mn} = a^{mn_1}$ .

That is  $a^{mn_1} = 1$ . Therefore, by theorem 1.4.5,  $n$  divides  $mn_1$ . Now since  $n$  and  $m$  are relatively prime,  $n$  and  $m$  are relatively prime,  $n$  divides  $n_1$ . But  $n_1 | n$  and  $n, n_1$  are positive integers, therefore  $n_1 = n$ . A similar argument shows that  $m = m_1$ . Thus  $\text{ord}(ab) = mn$ .

#### Theorem 1.4.8.

If  $G$  is a group and  $a \in G$  such that  $\text{ord}(a) = n$ ,  $\text{ord}(a^r) = m$  and  $d$  is the greatest common divisor of  $n$  and  $r$ , then  $m = n/d$ .

**Proof** Since  $d$  is the greatest common divisor of  $n$  and  $r$ , we can suppose that  $n = jd$  and  $r = kd$  where  $j, k$  are relatively prime. Then  $(a^r)^j = a^{rj} = a^{kdj} = a^{kn} = (a^n)^k = (1)^k = 1$  implies that  $m$  divides  $j$ . Also,  $1 = (a^r)^m = a^{rm} = a^{kdm}$  implies that  $n$  divides  $kdm$ . Since  $n = jd$ , we conclude that  $j$  divides  $km$ . Now,  $j, k$  are relatively prime, so  $j$  divides  $m$ . That is  $j = m$ . But  $n = jd$ . This shows that  $n = md$ . That is  $m = n/d$ .

Every group can be viewed as a subgroup of a bigger group. This suggests the importance of subgroups in Group Theory. The following section contains some basic results concerning subgroups.

## 5. SUBGROUPS OF A GROUP

If a group is extremely large in size (may be of infinite order) which is difficult to comprehend then one can reduce the group into a smaller group. There are several means of doing this, and one of these is the use of subgroups. The process can be reversed also. That is, larger groups can be constructed from smaller ones. In other words, a subgroup can be expanded to become a group of larger size. Some of these techniques will be studied later. In this section we introduce certain notions which we will require as the subject progresses.

A subgroup of a group  $G$  is a subset of  $G$  which itself forms a group with respect to the operation defining  $G$ . If  $H$  is a subgroup of  $G$ , we use W. Wielandt's notation to denote this fact by  $H \leq G$ . It is important to note that every group has at least two subgroups, namely  $\{1\}$  and  $G$ . The subgroup  $\{1\}$  is also called the trivial subgroup of  $G$ . A group  $G$  may or may not have subgroups other than the improper subgroup. If the group  $G$  has subgroups other than the improper ones, then such subgroups are called proper subgroups of  $G$ . If  $H$  is a proper subgroup of  $G$  then we denote it as  $H < G$ . Notice that every subgroup of an Abelian group is itself an Abelian group since its operations are necessarily all commutative. It is known now that the theory of Abelian groups is much simpler than that of groups in general, for the process of multiplication of the elements of such groups is commutative as well as associative.

Let us consider subgroups of certain important groups.

### Example 1.5.1

As an illustration, we will list all the subgroups of  $V_4 = \langle x, y : x^2 = y^2 = (xy)^2 = 1 \rangle$ . There are, in addition to the improper subgroups  $\{1\}$  and  $V_4$ , the following subgroups of  $V_4 : \{1, x\}, \{1, y\}, \{1, xy\}$ . Note that  $V_4$  has five subgroups in total and all of them except the improper ones are of order 2.

### Example 1.5.2

The group  $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$  has the following six subgroups:  $\{1\}, \{1, x\}, \{1, y, y^2\}, \{1, xy\}, \{1, xy^2\}, S_3$ . Note that  $S_3$  has proper subgroups of orders 2 and 3.

### Example 1.5.3

The set of rationals,  $\mathbb{Q}$ , is a subgroup of the additive group of real numbers.

**Example 1.5.4**

Let  $G$  be the group of all  $2 \times 2$  matrices  $\begin{bmatrix} x & y \\ z & w \end{bmatrix}$  with  $x, y, z, w \in R$  and  $xw - yz \neq 0$  under the matrix multiplication. Let  $H$  contain those matrices in  $G$  which are of the form  $\begin{bmatrix} x & y \\ 0 & w \end{bmatrix}$ . Then one can prove easily that  $H \leq G$ .

**Example 1.5.5**

Let  $C^x$  be the group of all non-zero complex numbers  $a+ib$ , where  $a, b \in R$ , under the multiplication defined as:  $(a+ib)(c+id) = (ac-bd) + i(ad+bc)$ . Then the subset  $H$  of  $C^x$ , containing the complex numbers  $a+ib$  such that  $a^2+b^2=1$  is a subgroup of  $C^x$ .

**Example 1.5.6**

Consider the group  $Z_4$  defined by the Cayley table:

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

The only subgroups of  $Z_4$  are:  $\{0\}, \{0,2\}$  and  $Z_4$ .

**Example 1.5.7**

The powers of any element of a finite group form a subgroup.

**Example 1.5.8**

The elements of finite order in an infinite Abelian group form a subgroup.

In the following we give several elementary results about subgroups of a group.

**Theorem 1.5.9**

Let  $H$  be a subset of a group  $G$ . Then  $H \leq G$  if and only if  $xy^{-1} \in H$ , for every  $x, y \in H$ .

**Proof.**

It is obvious that if  $H \leq G$  and  $x, y \in H$  then  $y^{-1} \in H$  and so  $xy^{-1} \in H$ . Note that  $H$  is non-empty because being a subgroup of  $G$  it contains at least one element, that is, the identity element.

Conversely, suppose that  $H$  is non-empty and  $xy^{-1} \in H$  for  $x, y \in H$ . In particular, for each  $x \in H$ ,  $xx^{-1} \in H$  implies that  $1 \in H$ . If we take  $x=1$  then  $xy^{-1} = 1y^{-1}$  implies that for each  $y \in H$  there exists  $y^{-1} \in H$ . That is  $xy \in H$ . The associative law for  $x, y, z$  in  $H$  holds because  $x, y, z$  are elements of  $G$ , in which the associative law certainly holds. This completes the proof.

### Corollary 1.5.10

Let  $H$  be a non-empty subset of a finite group  $G$ . Then  $H \leq G$  if and only if  $xy \in H$  whenever  $x, y \in H$ .

#### Proof.

If  $H \leq G$  then  $H$  is closed under the operation in  $G$ . Hence,  $x, y \in H$  implies that  $xy \in H$ .

Conversely, if  $x, y \in H$  implies that  $xy \in H$ , then obviously the closure property in  $H$  is satisfied. If  $x \in H$ , then  $x, xx, xxx, \dots$  are all in  $H$ , by hypothesis. But  $G$  is finite. Therefore for some positive integer  $n$ ,  $x^n = 1$ . Thus  $1 = x^n \in H$ . Finally, if  $x \in H$  then  $x^{-1} = x^{n-1} \in H$  for some  $n$ . Thus  $H \leq G$ .

### Theorem 1.5.11

If  $G$  is a group and  $H_i \leq G$  for all  $i$  in the indexing set  $I$ , then  $\bigcap_{i \in I} H_i \leq G$ .

#### Proof.

By making use of theorem 1.5.9, one can very easily prove that  $\bigcap_{i \in I} H_i \leq G$ .

The union of two subgroups of a group may not be a subgroup of the group. For instance, if we reconsider  $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ , we note that  $\{1, x\} \cup \{1, xy\}$  is not a subgroup of  $S_3$ . On the other hand, the group  $Z$  of integers under addition provides an illustration of theorem 1.5.11. It can be verified that the subsets  $\{n2^i : n = 0, \pm 1, \pm 2, \dots\}$  form subgroups for  $i = 1, 2, \dots$ . Their intersection is  $\{0\}$ , again a subgroup.

Let  $H$  and  $K$  be subsets of a group  $G$ . Then the product  $HK$  is defined as  $HK = \{hk : h \in H \text{ and } k \in K\}$ .

If  $H$  and  $K$  are subgroups then it is not necessary that  $HK$  will also be a subgroup. For example, if we consider the subgroup  $A = \{1, x\}$  and  $B = \{1, xy\}$  of  $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$  then  $AB = \{1, xy, x, y\}$ , according to example 1.5.2, is

not a subgroup of  $S_3$ . We will see in a little while that  $HK$  becomes a subgroup of  $G$  provided it satisfies a certain condition. First we prove the following lemmas.

**Lemma 1.5.12**

If  $H$  is any non-empty subset of a group  $G$  then  $HG = G = GH$ .

**Proof.**

By  $HG$  we mean  $\{hg : h \in H \text{ and } g \in G\}$ . Now  $x \in HG$  implies that  $x = hg$  for some  $h \in H$ . Since  $h \in H$  and  $H \subseteq G$  therefore  $h \in G$  and so due to closure property  $hg \in G$ . Thus,  $HG \subseteq G$ .

Conversely, if  $x \in G$  then  $x = h(h^{-1}x)$  where  $h \in H$ . Thus  $x = h(h^{-1}x) \in HG$  implies that  $G \subseteq HG$ . The two inclusions imply that  $HG = G$ . Similarly, we can prove that  $G = GH$ . This completes the proof.

**Lemma 1.5.13**

If  $G$  is a group and  $H \leq G, K \leq G$  then  $(HK)(HK) = HK$  provided  $HK = KH$ .

**Proof.**

Suppose  $HK = KH$ . Then  $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK)$ . But  $HH = H$  and  $KK = K$  by lemma 1.5.12. Thus  $(HK)(HK) = (HH)(KK) = HK$ .

**Theorem 1.5.14**

If  $G$  is a group and  $H \leq G, K \leq G$  then  $HK \leq G$  if and only if  $HK = KH$ .

**Proof.**

Suppose  $HK \leq G$  and  $x \in KH$ . This means that  $x = kh$  for some  $k \in K$  and  $h \in H$ . But  $x = kh = (k^{-1})^{-1}(h^{-1})^{-1} = (h^{-1}k^{-1})^{-1} \in HK$  because  $HK \leq G$ . Thus  $KH \subseteq HK$ . For the reverse inclusion, let  $x \in HK$ . Then  $x = y^{-1}$  for some  $y \in HK$  because  $HK$  is a group. Thus  $x = y^{-1} = (hk)^{-1}$  for some  $h \in H$  and  $k \in K$ . But  $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$  and so  $HK \subseteq KH$ . The two inclusions thus imply that  $HK = KH$ .

Conversely, suppose  $HK = KH$  and  $x, y \in HK$ . This means that  $y = hk$ , for some  $h \in H$  and  $k \in K$ . Hence  $y^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH$ . But  $KH = HK$  implies that  $y^{-1} \in HK$ . Thus  $xy^{-1} \in (HK)(HK)$  and so  $xy^{-1} \in HK$  because by lemma 1.5.13,  $(HK)(HK) = HK$ . Thus, by theorem 1.5.9,  $HK \leq G$ .

**Corollary 1.5.15**

If  $G$  is a group and  $H \leq G, K \leq G$  such that  $HK = KH$ , the group generated by  $H$  and  $K$  is equal to  $HK$ .

**Proof.**

Let  $\langle H, K \rangle$  denote the group generated by  $H$  and  $K$ . Then  $HK \subseteq \langle H, K \rangle$  because  $\langle H, K \rangle$  contains all products like  $hk$  where  $h \in H$  and  $k \in K$ . But  $H \subseteq HK$  and  $K \subseteq HK$  imply that  $\langle H, K \rangle \subseteq HK$  because  $HK \leq G$ . Hence, when  $HK$  is a subgroup of  $G$ ,  $HK = \langle H, K \rangle$ .

**Theorem 1.5.16**

If  $H, K$  are finite subgroups of a group  $G$ , then  $|HK| = \frac{|H||K|}{|H \cap K|}$ .

**Proof.**

If  $x \in H \cap K$  then  $x \in H$  and  $x \in K$  and so  $hx^{-1} \in H, xk \in K$  for some  $h \in H, k \in K$ . Thus  $hk = hx^{-1}xk \in HK$ . Thus each  $hk$  is repeated in the product  $HK$  at least  $|H \cap K|$  times as  $h$  runs through the elements of  $H$  and  $k$  runs through the elements of  $K$ . On the other hand, if  $hk = h'k'$  where  $h' = hx^{-1}$  and  $k'k^{-1} = (h')^{-1}h \in H \cap K$ . Put  $k'k^{-1} = (h')^{-1}h = x$ , then  $k' = xk$  and  $h' = hx^{-1}$ . Thus all repetitions are of the form given above. Hence each product  $hk$  is repeated precisely  $|H \cap K|$  times. This proves that  $|HK| = \frac{|H||K|}{|H \cap K|}$ .

In the following section, we explain one of the techniques through which subgroups can be used to construct a new group.

**6. DIRECT PRODUCTS**

To construct new structures from the known ones is one of the basic requirements of algebra. In this section we explain a simple and straightforward method by which we can construct a new group from the known groups.

We know that from any two sets  $X$  and  $Y$  we can construct another set  $X \times Y$ . This set is called the Cartesian product of  $X$  and  $Y$ . It contains the ordered pairs  $(x, y)$  where  $x \in X$  and  $y \in Y$ . For instance, the plane is a Cartesian product of the real line  $R$  with itself. If  $X$  and  $Y$  are finite sets then the size of  $X \times Y$  is the product of the sizes of  $X$  and  $Y$ .

Now if  $H$  and  $K$  are groups then the Cartesian product  $H \times K$  acquires the structure of a group under the operation of point wise multiplication. That is:

$$(h, k)(h', k') = (hh', kk') \text{ for all } (h, k), (h', k') \in H \times K.$$

The closure property is immediate from the definition of multiplication. The associativity follows from the associativity of multiplication in  $H$  and  $K$ . The element  $(1_H, 1_K)$ , where  $1_H$  denotes the identity in  $H$  and  $1_K$  denotes the identity in  $K$ , is the

identity in  $H \times K$ . For let  $(h, k)$  belong to  $H \times K$ ; then  $(h, k)(1_H, 1_K) = (h1_H, k1_K) = (h, k)$  and  $(1_H, 1_K)(h, k) = (1_H h, 1_K k) = (h, k)$ .

If  $(h, k) \in H \times K$  then the inverse of  $(h, k)$  is  $(h^{-1}, k^{-1})$  because  $(h, k)(h^{-1}, k^{-1}) = (hh^{-1}, kk^{-1}) = (1_H, 1_K)$  and  $(h^{-1}, k^{-1})(h, k) = (h^{-1}h, k^{-1}k) = (1_H, 1_K)$ . Thus we have shown that if  $H$  and  $K$  then  $H \times K$  is a group under the speation of pointers multipecelin.

Let us consider the following examples to illustrate the process of constructing a new group from two known groups.

### Example 1.6.1

We know that  $R$  is a group under addition. So  $R \times R$ , which is the complex plane, is also a group under addition.

### Example 1.6.2

Let  $C_2$  be the group of order 2 generated by an element  $x$ . That is,  $C_2 = \langle x : x^2 = 1 \rangle$ . Then the direct product  $G$  of  $C_2$  and  $C_2$  that is  $C_2 \times C_2$ , is the group  $\{(1, 1), (1, x), (x, 1), (x, x)\}$  under the operation of point wise multiplication. The element  $(1, 1)$  is the identity in  $G$  and each non-identity element is the inverse of itself. Note that  $G$  is an Abelian group and each non-identity element of  $G$  is of order 2 and  $|G| = 4$ . Due to these characteristics, we can say that the group  $G$  has resemblance with  $V_4$  because  $V_4$  too has the same characteristics.

### Example 1.6.3

Let  $C_2 = \langle x : x^2 = 1 \rangle$  and  $C_3 = \langle y : y^3 = 1 \rangle$ . Then  $C_2 \times C_3 = \{(1, 1), (1, y), (1, y^2), (x, 1), (x, y), (x, y^2)\}$ , the direct product of  $C_2$  and  $C_3$  is the group of order 6 in which  $(x, y)$  is of order 6. If we compare the two groups, of the same order, namely  $S_3$  and  $C_2 \times C_3$ , we observe that  $S_3$  has no element of order 6 whereas  $C_2 \times C_3$  has an element of order 6. Because  $C_2 \times C_3$  is Abelian whereas  $S_3$  is not. Thus, we can say that  $S_3$  and  $C_2 \times C_3$  are two different groups of the same order.

Notice that every group can be realized as the direct product of itself and the trivial group. Such a direct product is called the trivial direct product. If  $H$  and  $K$  are groups then every element of  $H \times K$  is expressible as the product of an element of  $H \times \{1\}$  and an element of  $\{1\} \times K$ . That is, if  $(h, k) \in H \times K$ , where  $h \in H$  and  $k \in K$ , then  $(h, k) = (h, 1)(1, k)$  where  $(h, 1) \in H \times \{1\}$  and  $(1, k) \in \{1\} \times K$ . That is,  $(h, 1)(1, k) = (h, k) = (1h, k1) = (1, k)(h, 1)$  for every  $(h, 1) \in H \times \{1\}$  and  $(1, k) \in \{1\} \times K$ . Furthermore, every element of  $H \times \{1\}$  commutes with  $\{1\} \times K$ . Observe that  $(H \times \{1\}) \cap (\{1\} \times K) = \{(1, 1)\}$  because  $x \in (H \times \{1\}) \cap (\{1\} \times K)$  then  $x = (h, 1) = (1, k)$  and the only solution for  $h, k$  is  $h = k = 1$ . That is,  $x = (1, 1)$ , it is fairly straightforward to see



that  $H \times K$  is Abelian if and only if  $H$  and  $K$  are Abelian groups. It is also easy to prove that  $H \times \{1\} \leq H \times K$  and  $\{1\} \times K \leq H \times K$ .

The definition of the direct product of two groups can be extended to the direct product of any finite number of groups. Suppose  $n$  is a positive integer and  $G_1, G_2, \dots, G_n$  be any  $n$  groups (not necessarily distinct as in example 1.6.2). Then  $G = G_1 \times G_2 \times \dots \times G_n$  is the set of all ordered  $n$ -tuples  $(x_1, x_2, \dots, x_n)$  where  $x_i \in G_i$  for  $i = 1, 2, \dots, n$ . The set  $G$  is a group under the operation  $(x_1, x_2, \dots, x_n)(y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$  where  $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in G$ . For instance, if  $V$  is an  $n$ -dimensional vector space over a field  $F$ , then  $V$  can be visualized as a direct product  $F \times F \times \dots \times F$  ( $n$ -times).

We closed this chapter with the following observations about the direct product of groups. If  $G$  is the direct product of groups  $G_1, \dots, G_n$  then  $G_i = \{1, 1, \dots, 1, x_i, 1, \dots, 1\} : x_i \in G_i\}$  is a subgroup of  $G$ . This subgroup  $G_i$  of  $G$  has some special properties which we will explain in some detail in the next chapter. Note that  $G = G_1 G_2 \dots G_n$  and every  $x \in G$  has a 'unique' presentation  $x_1 x_2 \dots x_n$  where  $x_i \in G_i$  for  $i = 1, 2, \dots, n$ . Sometimes the direct product is called external direct product, but throughout this book we will call it simply the direct product.

If  $G$  is a group and  $H \leq G, K \leq G$  then  $G$  is called the internal direct product of  $H$  and  $K$ , written as  $H \otimes K$ , if

- (i)  $hk = kh$  for every  $h \in H$  and  $k \in K$ , and
- (ii) every element  $x \in G$  can be uniquely written as a product of an element of  $H$  and an element of  $K$ .

## 7. EXERCISES

1. Draw a Cayley table for dihedral group  $D_4$ .
2. Prove that in the Cayley table of finite group, each element of the group appears once and only once in each row and column of table.
3. If  $G$  is finite group. Prove that for every  $g \in G$  there exist a positive integer  $r$  such that  $g^r = 1$ .
4. Find the order of the elements of  $Q_8$ .
5. Prove that  $Z_6$  is an Abelian group under addition. Determine all the subgroups of  $Z_6$ .

6. Prove that  $H = \{a + ib \in \mathbb{C} : a^2 + b^2 = 1\}$  is a subgroup of group  $\mathbb{C} - \{0\}$  under multiplication.
7. Determine the group generated by the symmetries of a square.
8. Show that a group  $G$  is Abelian if every element of  $G$  is its own inverse.
9. Let  $G$  be the set containing  $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  where  $a, b, c, d$  are integers modulo 2 such that  $ad - bc \neq 0$ . Prove that  $G$  is a group of order 6 under the operation of matrix multiplication.
10. Construct a new group with the help of  $C_2$  and  $V_4$ .
11. Define the internal direct product of  $C_2$  and  $C_2$ .
12. Find the order a group generated by the elements  $x, y$  satisfying the relations  $x^3 = y^2 = (xy)^2 = 1$ .
13. Show, by an example, that the converse of exercise 8 is not necessarily true.
14. Prove that the set  $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$  of residue classes modulo 8 forms a multiplicative Abelian group.
15. If  $G$  is a group, then prove that the identity element 1 is unique and the inverse of  $x \in G$  is unique.
16. If  $G$  is a group and  $a, b \in G$ , then prove that  $(ab)^{-1} = b^{-1}a^{-1}$  and  $(a^{-1})^{-1} = a$ .
17. If  $G$  is a group such that  $(ab)^2 = a^2b^2$  for all  $a, b \in G$ , then prove that  $G$  is Abelian.
18. Give an example of a group  $G$  in which  $(ab)^n \neq a^n b^n$  for some  $a, b \in G$  and a positive integer  $n$ .
19. Illustrate by an example that if  $H, K$  are subgroups of a group  $G$ , then
 
$$|HK| = \frac{|H||K|}{|H \cap K|}.$$
20. If  $G$  is a group, prove that  $ab$  and  $ba$  are of the same order for all  $a, b \in G$ .

21. Show that the group generated by  $a, b$  has fifteen elements if  $a^5 = b^3 = 1$  and  $ab = ba$ .